

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jamie Frates, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the Microsoft Corporation account: Harry_chavez@outlook.com that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation ("Microsoft"), an electronic communications company headquartered at Redmond, Washington. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government records and other information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer with the Federal Bureau of Investigation ("FBI"), and have been since July 2003. I am currently employed as a detective with the Kansas City, Missouri Police Department and am serving as a TFO with the FBI. I have been employed with the Kansas City, Missouri Police Department since July 2003, and am currently assigned to the FBI Child Exploitation Task Force, Kansas City, Missouri. Since February 2022, I have been assigned to investigate computer crimes to include violations against children. This includes violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have had numerous hours of professional law enforcement training in the detection and investigation of criminal offenses. I have written, executed, and/or

participated in the execution of numerous search warrants. Specifically pertaining to the area of child pornography and child exploitation investigations, I have gained expertise in these investigations through training, discussions with other law enforcement officers, and everyday work related to conducting these types of investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution of Child Pornography), have been committed by Harry Emanuel Chaves Flores. There is also probable cause to search the information described in Attachment B-I for evidence, instrumentalities, contraband, and/or fruits of these crimes as further described in Attachment B-II.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On November 4, 2022, Affiant was conducting an online investigation on the BitTorrent network for offenders sharing CSAM. Affiant directed his investigative focus to a device (“Suspect Device”) at IP address 136.34.111.237 because it was associated with torrents which were identified as having files of investigative interest to CSAM investigations. One of the

video files was labeled with the title “Kait 5yo”. The video was three minutes thirty-three seconds in length and depicted a naked from the waist down prepubescent female with an adult male who exposes her vagina and buttocks. The adult male then inserts his finger and his penis into her exposed vagina.

7. Between approximately November 4, 2022, and February 07, 2023, the Suspect Device had distributed a combination of over 5,000 CSAM videos and images over the BitTorrent network. One of the video files titled “Tara Buttfuck” depicted a prepubescent female being anally sodomized by an adult male. The video is approximately 33 seconds in length.

SUBJECT IDENTIFICATION

8. On November 4, 2022, Affiant conducted a query through MAXMIND, a digital mapping company that provides location data for IP addresses. MAXMIND reported that the Suspect Device at IP address 136.34.111.237, which was associated with Suspect Device, was registered to Google Inc. with a possible geo-location address in or near Kansas City, Missouri. On February 10, 2023, an administrative subpoena was served upon Google Inc., for subscriber information.

9. On February 17, 2023, Google’s response indicated that the subscriber information for IP address 136.34.111.237, which was associated with Suspect Device, was as follows: Harry Chavez, 525 East Armour Boulevard, Apt. 111, Kansas City, Missouri 64109-3027. The primary email address was harrychavezflores1995@gmail.com with an alternate email listed as harry_chavezf@icloud.com. A mobile phone number of 816-517-0133 was listed as a mobile phone number, associated with the account. The account activation date was on November 1, 2022. The first timestamp for the exact IP address was on November 1, 2022, and the last date stamp was February 16, 2023.

10. Law enforcement database searches revealed Harry Emanuel Chaves Flores (“Chavez Flores”), with a date of birth of July 14, 1995, Mexico passport number G41299959, was also associated with the above listed address. Information was also obtained that Chaves Flores was in the United States. on a Student and Exchange Visa for training at the Westin Crown Center Hotel, located in Kansas City, Missouri.

11. On March 31, 2023, Affiant obtained a federal search warrant from the Western District of Missouri for Chavez Flores’s residence, search warrant number 23-SW-00143-JAM. The search warrant was executed on April 3, 2023, at approximately 7:01 A.M. Central Time. Chavez Flores was present at the time the search warrant was executed, along with another adult male resident.

12. Affiant and TFO David Albers, FBI Kansas City, conducted an interview of the adult male resident. The other adult male resident advised that he had lived at the apartment since December of 2022, and that Chavez Flores was already established in the apartment upon his arrival. The male also confirmed that there were no other occupants. During the interview, a preview of this other adult male’s electronic devices determined that there was no CSAM on his devices, to which he had given his passwords/codes.

13. Affiant and Special Agent (“SA”) Alex Vance, FBI Kansas City, then conducted a voluntary interview of Chavez Flores. Chavez Flores advised that he had lived at the apartment since October of 2022 and confirmed that there were no other residents at the apartment. Chavez Flores identified his devices in the apartment, including a red iPhone 11 and a silver HP laptop to which he provided the access information. Chavez Flores admitted to using “Ares” (BitTorrent client), located on his HP laptop, which he stated that he used to download music or movies. Chavez Flores stated that he hasn’t used “Ares” for approximately a year. Chavez Flores stated

that he lived in the apartment by himself from October 2022 through part of December of 2022 until his roommate moved in. During his interview, a preview of Chavez Flores' laptop was conducted. Law enforcement located multiple video files were found within the "Ares" folder depicting CSAM on his laptop. Other file folders under the "Ares" program were found to be categorized with file names indicative of CSAM. These files contained videos and photographs of CSAM. The red iPhone 11 and silver HP laptop belonging to Chavez Flores were seized pursuant to the federal search warrant.

14. On April 3, 2023, a Cellebrite extraction was completed on the red Apple iPhone 11 belonging to Chavez Flores. The extraction revealed hundreds of CSAM images, including apparent screen shots from videos, located on the phone with at least 14 videos depicting CSAM. Also, law enforcement found messages on Chavez Flores' cell phone within the WhatsApp application. In these messages, Chavez Flores sent over 150 images of CSAM from November 10, 2022, through February 10, 2023, to unknown individuals via the application.

15. Chavez Flores' HP laptop was taken to the Heart of America Regional Computer Forensics Laboratory ("HARCFL") for a forensic examination. On May 9, 2023, Affiant picked up the HP laptop from HARCFL, after the completion of the examination, and obtained the results of their examination. The examination showed only a single user account, titled "harry," was the only user-generated account on the device. The examiner also identified over 900 unique pictures and over 880 unique videos featuring CSAM. The forensic examiner also determined that Harry_chavez@outlook.com ("TARGET ACCOUNT") is related to the possession of CSAM. The forensic examiner discovered apparent CSAM in two locations on the laptop computer associated with Microsoft cloud/internet storage, one of which was: [root]/Users/harry/OneDrive/ (Microsoft OneDrive).

16. Based on the information described above, Affiant believes that Microsoft user Harry_chavez@outlook.com is in fact Harry Chavez Flores' account ("TARGET ACCOUNT"). Affiant further believes there is probable cause that the Microsoft account Harry_chavez@outlook.com was used to store CSAM, based on the evidence the forensic examiner from HARCFL found during the forensic examination.

17. On April 25, 2023, a grand jury seated in the Western District of Missouri returned a two-count indictment against Chavez Flores, charging him with Distribution of Child Pornography over the Internet, in violation of 18 U.S.C. § 2252 (a)(2), and Possession of Child Pornography, in violation of 18 U.S.C. § 2252 (a)(4), in case number 23-00082-01-CR-W-SRB. An arrest warrant was issued the same day. When law enforcement went to execute the arrest warrant for Chavez Flores, it was discovered that he had previously absconded to Mexico, his country of origin. Chavez Flores remains in a fugitive status for this case in Mexico.

18. On June 13, 2023, a preservation letter was submitted to Microsoft, Inc. The preservation letter was submitted in reference to Harry_chavez@outlook.com ("TARGET ACCOUNT"). The preservation letter remains in effect.

INFORMATION ABOUT MICROSOFT

19. In my training and experience, I have learned that Microsoft provides a variety of online services, including electronic communications services, to the public. One such service is called Skype, which enables account holders the ability to send instant messages, text messages, multi-person group messages, image and file exchanges, video chats, video messages, voice calls, and multi-person conference calls, with other Skype users. Skype can be accessed either through a website or via the Skype application, which users can download and use on computers, tablets, cellular phones, certain televisions, and other electronic devices.

20. Microsoft (including Skype) subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved communications for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. A Microsoft subscriber can also store with the provider files in addition to Skype message files, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to messages), and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using a Microsoft (including Skype) account may be found in address books, contact or buddy lists, messages in the account, and attachments to messages, including pictures and files.

22. In my training and experience, electronic communications service providers generally ask their subscribers to provide certain personal identifying information when registering for an account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

23. In my training and experience, electronic communications service providers often maintain records of changes to the basic subscriber information of its accounts. This information may constitute evidence of the crimes under investigation because the information can show changes in ownership of the account or efforts to hide the identity of the account subscribers.

24. In my training and experience, providers like Microsoft typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, call detail records (*i.e.*, date, time, sender, receiver, duration of phone calls, text messages, and video messages), the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), device information associated with particular devices authorized and/or used to access the account, and other log files that reflect usage of the account. In addition, providers like Microsoft often have records of the Internet Protocol address ("IP address") used to register the account, the IP addresses associated with particular logins to the account, and the IP addresses used to send or receive particular messages. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a user's account.

25. In my training and experience, electronic communications service providers like Microsoft (including Skype) often also store and maintain the contents of the communications sent and/or received on their platforms, if the user account is configured to do so. This may include the text of instant messages and any images and/or video files attached to such messages, recorded voicemails, and other stored content. Such files can provide critical evidence of the crimes under

investigation, especially where, as here, the evidence indicates that the individuals under investigation used Skype to discuss the ongoing crimes.

26. In my training and experience, in some cases, users of services like Microsoft will communicate directly with the provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. As explained herein, information stored in connection with an electronic communications service account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with such accounts can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, electronic communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the provider can show how and when the account was accessed or used. For example, as described below, providers typically log the Internet Protocol (IP) addresses from which users access the account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can

understand the chronological and geographic context of the account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information in the account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications or making changes to the account's registration information in an effort to conceal information from law enforcement).

28. I know from my training and experience that Skype usernames can be associated with other Microsoft services such as OneDrive, a file hosting service that allows users to upload and sync files to a cloud storage and then access them from a Web browser or their local device, and Outlook and Hotmail, email service accounts.

29. I know from my training and experience; many electronic communications service providers maintain records of which accounts are "linked" either by common registration information or by "machine cookies." That is, the providers track for their own business purposes which accounts are accessed from the same electronic device, such as the same computer, through "machine cookies" (*i.e.*, small pieces of text sent to the user's device when visiting Microsoft). Providers likewise keep records of the accounts that share a common registration email address, telephone number, or IP address, or a common forwarding or recovery email address. The requested warrant would require Microsoft to identify any other accounts that are "linked" to the

Target Account, either by machine cookie or basic subscriber information and to disclose basic subscriber information for these “linked accounts.” *See* Attachment B I.H.

30. There is probable cause to believe that information stored in connection with this Microsoft Skype account will provide evidence of the “who, what, why, when, where, and how” for the dark web markets Skynet, Avior, and AlphaBay and their administrators and users.

31. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

32. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of violations, or attempted violations, of 18 U.S.C. § 2252, knowing distribution or possession of material involving the sexual exploitation of minors may be located in the Harry_chavez@outlook.com described in Attachment A.


33. Based on the foregoing, I request that the Court issue the proposed search warrant.

34. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft. Because the warrant will be served on Microsoft, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

35. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.


Respectfully submitted,



Jamie Frates
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me via reliable electronic means on 20th day of February 2024.

By telephone at 2:36 p.m.


HONORABLE JILL A. MORRIS
United States Magistrate Judge
Western District of Missouri



Assistant United States Attorney Ken Borgnino assisted in the preparation of this application for a search warrant. It was reviewed by Assistant United States Attorney Maureen Brackett.